Group Policy Object Processing Order

July 25, 2008

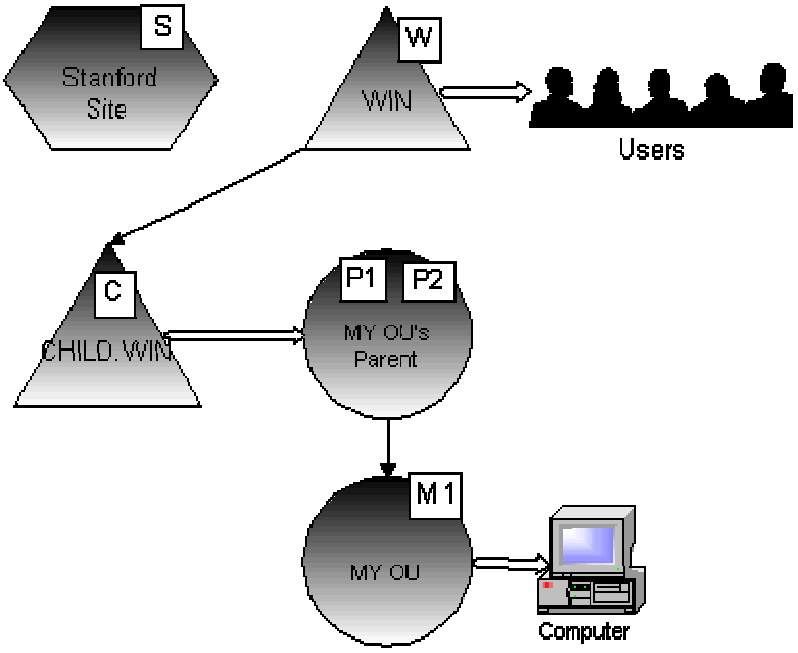
Introduction

To make clear GPO processing order.

Technical Information

GPOs are assigned to containers (sites, domains, or OUs). They are then applied to computers and users in those containers. GPOs can contain both computer & user sets of policies. The Computer section of a GPO is applied during boot-up. The User section of a GPO is applied at user login. User GPO processing can be configured three different ways, as documented below. Which processing order to use is determined by the GPO which is applied to the machine.

Example:



Normal mode	Loopback: Merge mode	Loopback: Replace mode
GPOs assigned to local machine during boot (Computer sections of the policy) Local Machine Policy Site GPOs **[S]** Domain GPOs **[C]** OU GPOs **[P1,P2,M1]**	**GPOs assigned to local machine during boot** (Computer sections of the policy) Local Machine Policy Site GPOs **[S]** Domain GPOs **[C]** OU GPOs **[P1,P2,M1]**	**GPOs assigned to local machine during boot** (Computer sections of the policy) Local Machine Policy Site GPOs **[S]** Domain GPOs **[C]** OU GPOs **[P1,P2,M1]**
GPOs assigned to user during logon (User sections of the policy) Local Machine Policy Site GPOs **[S]** Domain GPOs **[W]** OU GPOs **[]**	**GPOs assigned to user during logon** (User sections of the policy) Local Machine Policy {From User location} Site GPOs **[S]** Domain GPOs **[W]** OU GPOs **[]** {From Computer location} Site GPOs **[S]** Domain GPOs **[C]** OU GPOs **[P1,P2,M1]**	**GPOs assigned to user during logon** (User sections of the policy) Local Machine Policy {From Computer location} Site GPOs **[S]** Domain GPOs **[C]** OU GPOs **[P1,P2,M1]**

- **Detailed Computer Configuration Application Order:** Windows NT System Policies, if the computer is a member of a Windows NT 4.0 Domain that uses them, are applied first. Then Windows 2000 GPOs are applied, starting with Local GPO - This is the only one if the computer is in a Windows NT 4.0 Domain.

Detailed User Configuration Application Order: Mandatory/Roaming Profile, if present, is applied first. Then Windows NT ntuser.pol is applied if the user is from a Windows NT 4.0 Domain that uses System Policy. Then Windows 2000 GPOs are applied, starting with Local GPO.

Group Policy Loopback Support as described in MS whitepaper:

Group Policy is applied to the user or computer, based upon where the user or computer object is located in the Active Directory. However, in some cases, users may need policy applied to them, based upon the location of the computer object, not the location of the user object. The Group Policy loopback feature gives the administrator the ability to apply Group Policy, based upon the computer that the user is logging onto.

To describe the loopback feature, we'll use an example. In this scenario, you have full control over the computers and users in this domain because you have been granted domain administrator rights.

The following illustration shows the Streetmarket domain, which is used to work through this example.

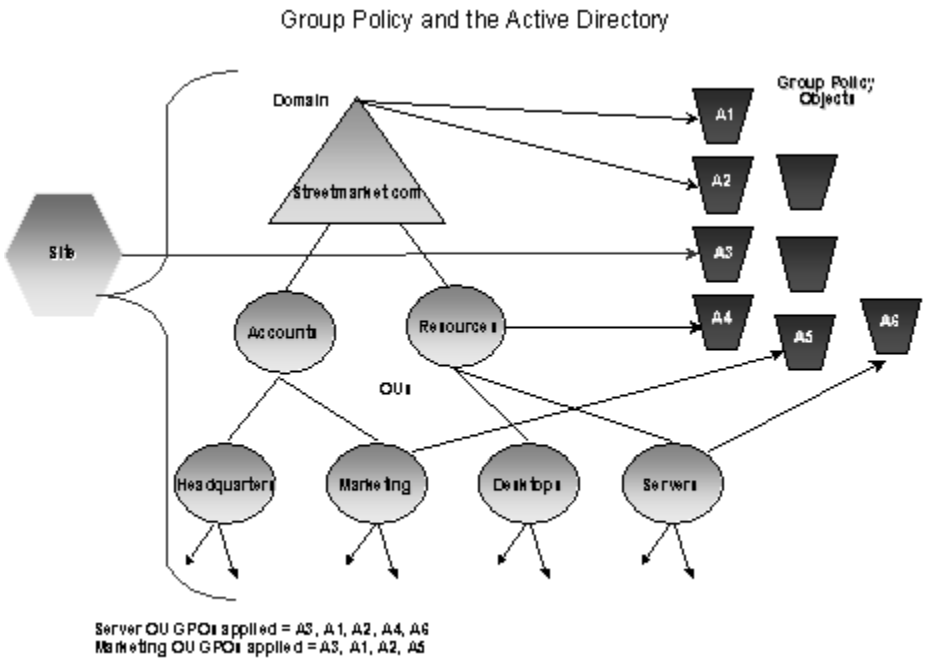


Figure 8. The Streetmarket domain

When users work in their own workstations, they should have Group Policy applied to them according to the policy settings defined, based on the location of the *user* object. However, when users log on to a computer whose computer object is in the in the Servers OU, they should get user policy settings based on the *computer* object location, rather than the user object location.

Normal user Group Policy processing specifies that computers located in the Servers OU have the GPOs A3, A1, A2, A4, A6 applied (in that order) during computer startup. Users of the Marketing OU have GPOs A3, A1, A2, A5 applied (in that order), regardless of which computer they log on to.

In some cases this processing order may not be appropriate, for example, when you do not want applications that have been assigned or published to the users of the Marketing OU to be installed while they are logged on to the computers in the Servers OU. With the Group Policy loopback support feature, you can specify two other ways to retrieve the list of GPOs for any user of the computers in the Servers OU:

Merge mode. In this mode, during logon the user's list of GPOs is gathered normally by using the **GetGPOList** function, and then **GetGPOList** is called again using the computer's location in the Active Directory. Next, the list of GPOs for the computer is added to the end of the GPOs for the user. This causes the computer's GPOs to have higher precedence than the user's GPOs. In this example, the list of GPOs for the computer is A3, A1, A2, A4, A6, which is added to the user's list of A3, A1, A2, A5 which results in A3, A1, A2, A5, A3, A1, A2, A4, and A6 (listed in lowest to highest priority).

Replace mode. In this mode, the user's list of GPOs is not gathered. Only the list of GPOs based upon the computer object is used. In this example, the list is A3, A1, A2, A4, and A6.

The loopback feature was implemented in the Group Policy engine1[1], not in the **GetGPOList** function. When the Group Policy engine is about to apply user policy, it looks in the registry for a computer policy, which specifies which mode user policy should be applied in. Then, based upon this policy, it calls **GetGPOList**, as appropriate.